(Following Paper ID and Roll No. to be filled in your Answer Books)

PAPER ID : ME25

Roll No. | | | | | | | | | | |

M. TECH. (Sem.II)

THEORY EXAMINATION 2015-16

ADVANCED NETWORK SECURITY

Time: 3 Hours Total Marks: 100

Note- Attempt All Questions. All Questions carry equal marks.

1. Attempt any four of the following:- (5×4=20)
   (a) What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Justify your answer.
   (b) What is an important difference between a symmetric-key system and a public-key system?
   (c) Consider an 8-block cipher. How many possible input blocks does this cipher have? How many possible mappings are there?
   (d) Explain what factors influence the strength of an encryption key.
   (e) Why are hash functions for digital signatures and what factors makes a hash function secure?

(f) In what way does the public-key encrypted message hash provide a better digital signature than the public-key encrypted message?

2. Attempt any two of the following:- (10×2=20)

(a) Discuss Massey-Omura Elliptic Curve Cryptosystem.

(b) Describe Elliptic Curve Discrete Logarithm Problem.

(c) Explain strength analysis of elliptic curve encryption and decryption.

3. Attempt any two of the following:- (10×2=20)

(a) What do you understand quantum cryptography? Discuss its limitations and challenges.

(b) Which cryptographic functionalities can be achieved by quantum protocols? Does quantum information allow for devices that hide the inner workings of a computer program?

(c) What are the limits of the delegated quantum computation scenario? What are the limits of the delegated quantum computation scenario?

4. Attempt any two of the following:- (10×2=20)

(a) How web security can be achieved? Explain the operation of SSL Record protocol with a neat diagram.

(b) Define the three classes of intruders and mention the intrusion techniques to protect from the intruders. Explain the different types of viruses.

(c) Discuss the various application services and security protocols used in e-Commerce.

5. Attempt any two of the following:- (10×2=20)

(a) What are the strength and weakness of firewalls. Discuss the secure firewall with IP packet screen router.

(b) What do you understand by standard VPN technique? Explain

(c) Describe classic security model of the operating system? What are the international standards for operating system security?

*****